

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 926 601 A1

(12)

## EUROPEAN PATENT APPLICATION

(43) Date of publication:

30.06.1999 Bulletin 1999/26

(51) Int. Cl.<sup>6</sup>: G06F 12/14, G11C 8/00,  
G11C 16/06, G07F 7/10

(21) Application number: 97830717.1

(22) Date of filing: 24.12.1997

(84) Designated Contracting States:

AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC  
NL PT SE

Designated Extension States:

AL LT LV MK RO SI

(71) Applicant:

STMicroelectronics S.r.l.  
20041 Agrate Brianza (Milano) (IT)

(72) Inventors:

- Campardo, Giovanni  
24100 Bergamo (IT)

• Ghezzi, Stefano  
24048 Treviolo (Bergamo) (IT)

• Giannini, Giuseppe  
20041 Agrate Brianza (Milano) (IT)

• Torricelli, Piero Enrico  
20040 Cavenago Brianza (Milano) (IT)

(74) Representative: Botti, Mario  
Botti & Ferrari S.r.l.

Via Locatelli, 5  
20124 Milano (IT)

(54) Data protection method for a semiconductor memory and corresponding protected memory device

(57) The invention relates to a method of protecting data in a semiconductor electronic memory comprising a memory matrix (2) and respective matrix address decoding (3) and predecoding (4) blocks. The method consists of using a protected memory portion (5) within said matrix (2) and respective dedicated decoding portions (6,7) for storing, into the protected portion (5), a protection code (CP) external to the address area of the matrix (2).

The protection code (CP) can only be written and/or read through a command interpreter (8).

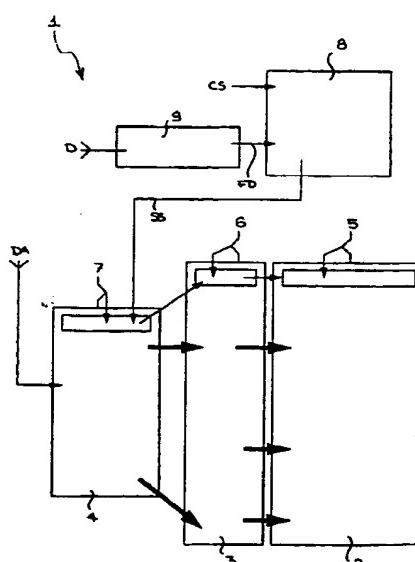


FIG. 1

EP 0 926 601 A1

**Description****Field of the Invention**

[0001] This invention relates to a method of protecting data in a semiconductor electronic memory having a memory matrix and respective matrix address decode and pre-decode blocks.

[0002] The invention also relates to a semiconductor electronic memory device having a protection function for the data stored therein, and being of a type which comprises a memory matrix and respective matrix address decode and pre-decode blocks.

[0003] Semiconductor memories are used in apparatus of ever more sophisticated design and expanding acceptance which require protection for the data stored therein.

[0004] The term "protection" may either encompass:

- protection from unintentional writing or erasing; or
- protection from tampering in order to extract or modify the memory contents.

[0005] The invention is particularly, but not exclusively, concerned with the latter type of protection, and the ensuing description will cover this field of application for convenience of explanation.

**Prior Art**

[0006] As is known, in semiconductor memories, conditional access must be provided to certain memory portions. An ability to defeat deceptive attempts carried out by reading from the interdicted areas of such memories is of paramount importance. For example, data relating to the protection code CP of the memory would be stored in such areas.

[0007] On the other hand, semiconductor memories have other areas where information is stored which can be read and/or modified in the usual manner. Thus, the situation is one where different memory areas may or may not be conceded to reading.

[0008] In addition, a semiconductor memory usually includes areas containing program instructions to be executed.

[0009] The simplest way of providing a safety feature consists of using a decoding code DEC, also known as the access or identification code, which usually comprises a few bytes or memory words. Without this decoding code, no consistent data can be read from the memory, nor can the contents of previously stored data be modified.

[0010] Thus, the location Xdec of the decoding code DEC is critical to the achievement of improved safety for a semiconductor memory.

[0011] In particular, the location Xdec of the decoding code DEC should meet certain basic requirements, as

follows:

it should be a read-only area, or at least an area which is only intelligible to the manufacturer in possession of the decoding code DEC;

- it should be an unmodifiable area under any conditions of the memory operation;
- it should be an area readily accessible at the fabrication stage and later on for servicing.

[0012] It should be considered, in fact, that the memory write time is a critical parameter at its fabrication stage. In particular, providing easily accessed memories is important if this write time is to be reduced.

[0013] A first prior approach to filling this demand consisted of using some memory locations of unknown address whereinto the bytes of the protection code CP could be stored. The reliability of this prior method is dependent on two features:

- the address whereat the protection code CP has been stored is unknown; and
- in any event, the data stored at that address cannot be interpreted directly.

[0014] However, this first protection method has certain unfavorable features which make it complicated to apply and lower its safety level.

[0015] In conventional semiconductor memories, these memory locations for the bytes of the protection code CP can only be provided within a memory array shared with the data. It is, therefore, necessary to use a software program for the write step which can memorize and avoid memory bits already in use.

[0016] However, the problem arises of how to erase the whole memory, or whole sections thereof which might contain bytes of the protection code CP. This problem is intensified in the instance of semiconductor memories of the flash type.

[0017] In this situation, the erase operation must be preceded by a temporary saving of the memory protection code CP. For the purpose, a temporary or buffer memory may be used wherfrom the protection code CP can later be read for re-writing to the bytes reassigned thereto.

[0018] Consequently, a protection method of that type tends to complicate both the hardware and the software of the semiconductor memory. In particular, the step of copying the protection code CP during the semiconductor memory fabrication process represents an unacceptable waste of time in such applications as cellular phones.

[0019] Furthermore, since the bytes of the protection code CP are written and erased using standard commands, anybody would be able to damage or read the

protection code CP contained therein, and possibly fully interpret it without the decoding code DEC.

[0020] A truly effective data protection method should be based on the following considerations:

it is convenient that the address space reserved for the protection code CP locates outside the memory array whereinto standard data is written;

it is necessary that the protection code CP can be written only once, and cannot be erased;

it is of advantage that different write/read procedures be used which differ, but not to a substantial extent, from standard; in fact, slightly modified write/read procedures would allow a managing software to be used which is basically similar as that used for standard operations.

[0021] The technical problem underlying this invention is to provide a data protection method for semiconductor memories, and a protected memory configuration, which have such structural and functional features as to overcome the drawbacks of prior protection methods and semiconductor memories, in the light of the foregoing reflections upon providing a memory device with an effective protection.

#### Summary of the Invention

[0022] The principle of this invention is a protection method which utilizes an OTP (One Time Programmable) memory area, and can meet all of the above requirements regarding safety, reliability, and ease of access, for a protected memory configuration in accordance with the method.

[0023] Specifically, the protection method of this invention uses a small, suitably configured portion of the standard memory array, and only requires that two extra instructions be added to the standard instruction sequence for the memory read/write operations.

[0024] Based on this principle, the technical problem is solved by a data protection method as previously indicated and defined in the characterizing portion of Claim 1.

[0025] The problem is also solved by a memory device for implementing the inventive method, as previously indicated and defined in the characterizing portion of Claim 5.

[0026] The features and advantages of the protection method and memory device according to the invention will be apparent from the following description of a non-limiting embodiment thereof, given with reference to the accompanying drawings.

#### Brief Description of the Drawings

[0027] In the drawings:

5 Figure 1 shows a protected memory configuration implementing the data protection method of the invention.

#### Detailed Description

[0028] Referring to the drawing figure, generally and schematically shown at 1 is a semiconductor memory device having a memory matrix or configuration 2 according to this invention.

15 [0029] The semiconductor memory device 1 also includes a decoding block 3 having its output connected to the memory matrix 2 and its input connected to a pre-decoding block 4 which is input memory addresses DA to be accessed.

20 [0030] In particular, the memory configuration 2 includes a protected OTP memory area 5 connected to first 6 and second 7 special decoding zones for the protected memory area 5. The first and second special decoding zones, 6 and 7, are connected in the decoding block 3 and the pre-decoding block 4, respectively.

25 [0031] The semiconductor memory device 1 further includes a command interpreter 8 which is input control signals CS and suitably filtered data values FD.

[0032] Advantageously in this invention, these suitably 30 filtered data values FD are produced from a programmable code filter 9 which is input the original data D.

[0033] In addition, the command interpreter 8 outputs a selection signal SS which is connected to the protected OTP memory area 5 through a series of the first 35 and second special decoding zones 6 and 7.

[0034] A protected memory configuration according to the invention basically comprises the combination of the memory configuration 2, itself comprised of the protected OTP memory area 5 and the first 6 and second 7 special decoding zones, and the programmable code filter 9.

[0035] Thus, the data protection method of this invention involves the use of a protected OTP memory area additionally to the standard data memory array in the 40 semiconductor memory device 1.

[0036] The size of this additional area 5 is dependent on the number of bytes used for storing the protection code CP. For example, in a cellular phone type of application, OTP memory rows could be introduced into the 45 memory matrix 2 and in part used directly by the manufacturer to counteract the serious problem of "clonation".

[0037] The data protection method of this invention further comprises the addition of two instructions, which 50 can be interpreted by the command interpreter 8, specifically an OTP read instruction ("read OTP data") and an OTP program instruction ("program OTP data"), no erase instruction being provided for the protected OTP

memory area 5.

[0038] Advantageously in this invention, these read and program OTP instructions may differ to suit individual customer's requirements.

[0039] The decoding code DEC comprises essentially these particular instructions for the protected OTP memory area 5.

[0040] In summary, the data protection method, and corresponding protected memory configuration, according to the invention afford the following advantages:

the protection code CP stored in the protected OTP memory area cannot be lost, does not belong to the standard address area of the memory array, and can only be read and/or written if the appropriate instructions are known; this provides a high safety level for the protection code CP;

at the designing stage, the protected OTP memory area will require some additional elements (rows and/or columns) involving a trivial (zero, for cellular phone applications) increase in memory area occupation, and permit the use of standard decoding methods; accordingly, no additional address bits will be required, the OTP read and program instructions re-addressing the address bus;

the command interpreter 8 can be re-programmed through the programmable code filter 9; this allows the OTP read and program instructions to be customized, thereby raising the safety level of the protection code CP even further;

by using only slightly modified OTP read and program instructions, existing circuitry (such as the decoding block 3, pre-decoding block 4, and command interpreter 8) in the semiconductor memory device can be utilized.

[0041] The solution illustrated in relation to the protection code CP of a semiconductor memory device 1 can also be used for any data to be stored on a permanent basis. Such data, therefore, should remain unaltered even after the whole memory array containing it has been erased.

[0042] Where the solution proposed by this invention is used, it becomes unnecessary to save the permanent data prior to erasing in order to have it restored at the end of the erase operation.

decoding portions (6,7) for storing, into said protected portion (5), a protection code (CP) without the address area of the matrix (2).

5 2. A method according to Claim 1, characterized in that said protection code (CP) can only be written and/or read through a command interpreter (8).

10 3. A method according to Claim 1, characterized in that said protected memory portion (5) is of the OTP type.

15 4. A method according to Claim 1, characterized in that said protection code (CP) can be written and/or read using a decoding code (DEC).

5 5. A semiconductor electronic memory device (1), having a protection function for the data stored therein and being of a type which comprises a memory matrix (2) and respective matrix address decoding (3) and pre-decoding (4) blocks, characterized in that it comprises:

20 25 a protected memory portion (5) incorporated to said matrix and associated with respective dedicated decoding portions (6,7);

25 a command interpreter (8) being input control signals (CS) and having its output coupled to said protected memory portion (5);

30 a programmable code filter (9) having a data input (D) and an output connected to an input of the command interpreter (8).

35 6. A device according to Claim 5, characterized in that said protected memory portion (5) is of the OTP type.

40 7. A device according to Claim 5, characterized in that said dedicated decoding portions (6,7) are incorporated to the decoding block and the pre-decoding block, respectively.

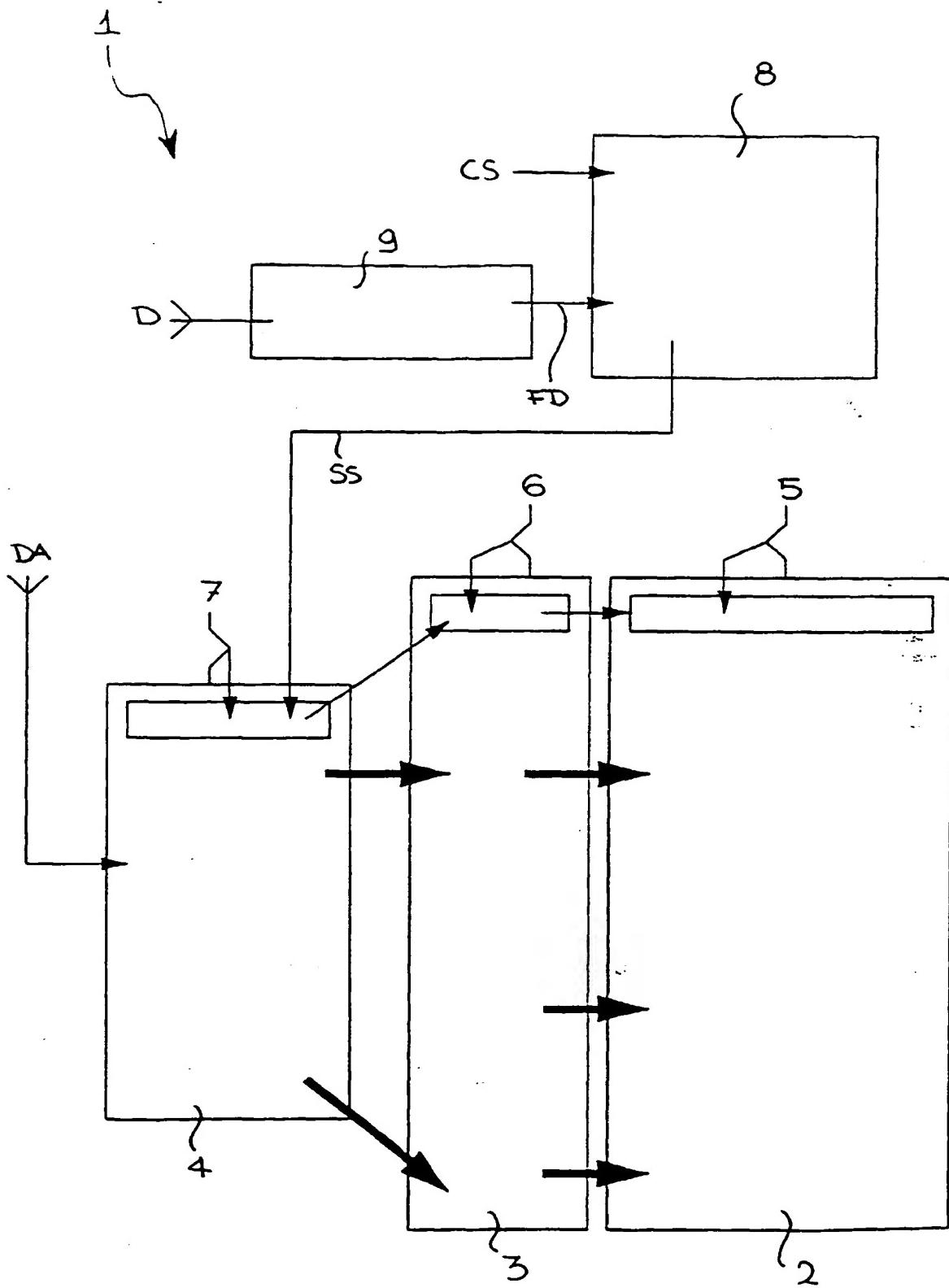
45 8. A device according to Claim 5, characterized in that the output from the command interpreter (8) is coupled to said protected memory portion (5) through a series of said dedicated decoding portions (6,7).

50

55

## Claims

1. A method of protecting data in a semiconductor electronic memory comprising a memory matrix (2) and respective matrix address decoding (3) and pre-decoding (4) blocks, characterized in that it consists of using a protected memory portion (5) within said matrix (2) and respective dedicated

**FIG. 1**



European Patent  
Office

## EUROPEAN SEARCH REPORT

Application Number

EP 97 83 0717

DOCUMENTS CONSIDERED TO BE RELEVANT			CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	
A	US 5 206 938 A (FUJIOKA SHUZO) 27 April 1993 * abstract; figures 3,4A,4B * * column 2, line 60 - column 3, line 2 * ---	1-8	G06F12/14 G11C8/00 G11C16/06 G07F7/10
A	US 4 744 062 A (SAWASE TERUMI ET AL) 10 May 1988 * the whole document * ---	1-8	
A	US 5 434 999 A (GOIRE CHRISTIAN ET AL) 18 July 1995 * abstract * * column 1 - column 28, line 68 * ---	1-8	
A	US 5 691 945 A (LIOU KONG-MOU ET AL) 25 November 1997 -----	1-8	
The present search report has been drawn up for all claims			TECHNICAL FIELDS SEARCHED (Int.Cl.6)
			G06F G11C G07F
Place of search		Date of completion of the search	Examiner
THE HAGUE		27 August 1998	Powell, D
CATEGORY OF CITED DOCUMENTS			
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document			
T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

**ANNEX TO THE EUROPEAN SEARCH REPORT  
ON EUROPEAN PATENT APPLICATION NO.**

EP 97 83 0717

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on. The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

27-08-1998

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5206938	A	27-04-1993	JP 2293196 A JP 2682700 B FR 2646942 A GB 2232281 A, B	04-12-1990 26-11-1997 16-11-1990 05-12-1990
US 4744062	A	10-05-1988	JP 61245255 A JP 61249156 A JP 62008397 A US 4821240 A US 4920518 A US 4974208 A	31-10-1986 06-11-1986 16-01-1987 11-04-1989 24-04-1990 27-11-1990
US 5434999	A	18-07-1995	FR 2638868 A AT 164249 T CA 2002349 A, C DE 68928608 D DE 68928608 T DK 165390 A EP 0368752 A ES 2114852 T WO 9005347 A JP 7048178 B JP 3500827 T NO 300438 B	11-05-1990 15-04-1998 09-05-1990 23-04-1998 16-07-1998 22-08-1990 16-05-1990 16-06-1998 17-05-1990 24-05-1995 21-02-1991 26-05-1997
US 5691945	A	25-11-1997	WO 9638845 A EP 0829086 A	05-12-1996 18-03-1998

**THIS PAGE BLANK (USPTO)**